WHAT IS CLAIMED:

1. A method for encrypting a data file content, the method comprising the steps of:

encrypting the data file with a master key;

generating one or more dual-encrypted blocks based on a set of secondary keys, the dual-encrypted blocks contained within the encrypted data file; and

providing the encrypted data file and an attachment file to an authorized user, the attachment file enabling a device to access the data file content once for each secondary key.

2. The method of claim 1 further including the steps of:

randomly generating the master key; and

hiding the master key within a data structure of the attachment file.

3. The method of claim 2 further including the steps of:

creating an odd logarithmic bit integer; and

incrementing the integer by two until a prime number is found;

said prime number defining the master key.

4. The method of claim 2 further including the step of using an NP-hard problem to hide the master key.

5. The method of claim 1 further including the steps of:

selecting one or more continuous blocks to be dual-encrypted;

randomly generating the secondary keys;

generating a duplicate selected block for each secondary key in the set;

generating dual-encrypted blocks based on the duplicate selected blocks and the secondary keys;

inserting the dual-encrypted blocks into the data file.

6. The method of claim 5 further including the steps of:

encrypting the secondary keys with the master key;

formatting the encrypted secondary keys as a data structure; and

storing the data structure in the attachment file.

7. The method of claim 6 further including the steps of:

encrypting a first secondary key with the master key; and

encrypting subsequent secondary keys in the set with all preceding secondary keys in the set.

8. The method of claim 1 further including the steps of:

receiving an email message from the attachment file, the message having a status content unique to the attachment file; and

determining whether another message having the status content has already been received.

9. The method of claim 8 wherein the status content defines a current operational state and an identifier for the attachment file.

10. The method of claim 8 further including the step of storing the status content to a data storage medium.

11. A method for enabling a device to access an encrypted data file content, the method comprising the steps of:

decrypting single-encrypted blocks of the data file with a master key;

decrypting dual-encrypted blocks of the data file with the master key and a secondary key; and

repeating the decryption steps for a set of secondary keys such that the device is able to access the data file content once for each secondary key in the set.

12. The method of claim 11 further including the step of decrypting the blocks on a block-by-block basis such that the device only has access to the data file content one block at a time.

13. The method of claim 12 further including the step of re-encrypting the single-encrypted blocks with a new master key.

14. The method of claim 13 further including the steps of:

randomly generating the new master key; and

hiding the new master key within a data structure.

15. The method of claim 14 further including the steps of:

creating an odd logarithmic bit integer; and

incrementing the integer by two until a prime number is found;

said prime number defining the new master key.

16. The method of claim 14 further including the step of using an NP-hard problem to hide the new master key.

17. The method of claim 12 further including the step of discarding the dual-encrypted blocks after decryption with the secondary keys.

18. The method of claim 11 further including the step of transmitting an email message to a provider of the encrypted data file, the message having a status content.

19. The method of claim 11 further including the step of adding footprint files to a host system, the footprint files enabling detection of copying of the encrypted data file.

20. The method of claim 11 further including the step of adding footprint data to files contained on a host system, the footprint data enabling detection of copying of the encrypted data file.